6-2023

Understanding and Applying SAR to Ideological and Nation- State-Sponsored Cybercrimes

Thomas J. Holt

Steve Chermak

Joshua D. Freilich

Emily Greene-Colozzi

National Counterterrorism Innovation, Technology, and Education Center

Understanding and Applying SAR to Ideological and Nation-State-Sponsored Cybercrimes

Thomas J. Holt, Steve Chermak,
Joshua D. Freilich, Emily Greene-Colozzi

MICHIGAN STATE UNIVERSITY
JOHN JAY COLLEGE OF CRIMINAL JUSTICE
UMASS LOWELL

NCITE NATIONAL COUNTERTERRORISM, INNOVATION, TECHNOLOGY, AND EDUCATION CENTER
A U.S. DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

The use of computer hacking, malicious software, and other forms of cyberattacks against U.S. infrastructure has increased dramatically since the 1990s. Many of these attacks target corporations and individuals for instrumental economic gain, such as the theft of personal information for use in fraud. Ideologically motivated attacks also occur, though the degree to which they are understood or documented is generally limited. For instance, jihadi groups have expressed an interest in cyberattacks since the early 2000s (see Holt et al., 2022). Similarly, DHS (2009) noted in the late 2000s that they expected cyberattacks from environmental or animal liberation-focused groups to increase. Attacks not only originate from individual actors, but also from nation-state-sponsored actors who seek to further the political and economic interests of their governments.

Given the lack of research and insights into the practices of ideological cyberattackers, this project seeks to understand the degree to which ideological cyberattacks occur and whether traditional indicators for suspicious activity reporting (SAR) are present for these incidents. There is a specific need to address SAR as it is unclear whether traditional risk factors for offline activity, such as the stockpiling of weapons or publication of manifestos, relate to cyberattacks. This analysis will specifically focus on the extent to which SAR indicators could be identified across ideological attacks against U.S. infrastructure, originating from nation-states or non-nation-state-sponsored actors.

To develop the data for this analysis, the researchers utilized the Extremist CyberCrime Database (ECCD), an open-source data set utilizing definitional frameworks that mirror other open-source databases for off-line terror, violence, and extremist-related crime, especially the U.S. Extremist Crime Data Base (Freilich et al., 2014). The database includes a purposive set of incidents occurring between January 1, 1998, and December 31, 2018. An open-source search protocol was developed that covered over 80 different sources, including media reporting, cybersecurity vendor reports, law enforcement and government materials, academic research, blog sites, and watch group reports (see Holt et al., 2022 for more detail).

All incidents included must have targeted either a) internet infrastructure physically hosted in the United States (U.S.) or b) targets operating within the United States (i.e., American companies or citizens). Additionally, all ideological frameworks are included in this data, along with incidents that were performed by nation-state-sponsored attackers such as Russian or Chinese military actors.

The ECCD also captures cyberattacks as "schemes," which can involve a single incident or series of attacks motivated by the same ideological cause or purpose performed against any number of targets over time (Freilich et al., 2014). This enables all incidents within a larger attack to be captured and coded to reflect the variations in attacker behavior, target preferences, and success rates. This methodology provided a final sample of 246 incidents occurring between 1998 and 2018. Due to missing data across these incidents, our final sample to assess for SAR indicators consisted of 196 total cyberattacks.

The research team developed a series of suspicious activity reporting measures based on published research and open reporting on indicators used by DHS, FBI, and FinCen requirements. A total of 177 indicators were created and were applied to the corpus of open-source reporting developed within the ECCD (available upon request). The research team then coded the data for the presence of each indicator within the 196 cyberattacks included in the final sample.

Our analysis demonstrates that the majority of indicators (113) were either absent in open-source reporting or not attributable to the attacks. Of the remaining 64 measures where information could be found to support the indicator, those with the greatest frequency were not necessarily unique or demonstrable evidence of risk for ideologically motivated cyberattacks. For instance, group associations (n=127), hacking attempts (n=111), and joining or creating groups (n=95) were the most common indicators identified across all cases in the sample (see table below). These are common practices among hackers generally and would not serve as critical indications of risk for involvement in an ideologically motivated cyberattack.

A smaller portion of attackers engaged in activities to conceal their technology use activities (n=59) and engaged in active research and planning to commit cyberattacks (n=59). Involvement in breaches of similar targets were somewhat common (n=56), though acts of fraud (n=43) and economic cybercrime (n=38) were less common. The use of money laundering was uncommon (n=17) as were acts of financial manipulation (n=13) and theft or diversion prior to the incident (n=10). A small proportion of individuals engaged in activities like evading law enforcement (n=25), presenting false information (n=23) and false identification (n=21) to gain access to sites, and the use of social engineering in physical space (n=14).

It should be noted that communications with violent extremists were observed among a small proportion of actors (n=29), most of whom performed ideologically motivated cyberattacks without state sponsorship (n=22). Similarly, encouraging violence and producing violent media content were somewhat uncommon (n=17).

More serious measures for suspicious financial activities and behavioral changes were largely absent from open reporting. For example, suspicious cryptocurrency transfers were only present in seven cases, and suspicious Western Union/MoneyGram transactions were present in five cases. Suspicious credit and debit card activities were only present in three cases, all of which were associated with nation-state actors. Only one instance of support for terrorist financing was observed, which was associated with a nation-state sponsored actor. Suspicious travel was observed in eight instances, almost all of which were associated with nation-state actors (n=7).

Activities related to physical conflict actions were very rare, such as building explosives (n=1), or acquiring weapons (n=1). Performing physical damage to targets was observed in 10 total cases, though they were all associated with ideologically motivated actors without state sponsorship. Travel preparation or a desire to travel were also exceedingly uncommon (n=1).

Taken as a whole, this analysis demonstrates that the SAR measures traditionally used for real world extremist activity do not appear as often in ideologically motivated cyberattacks. The financial activity measures may be relevant, though they are not as common in this sample of actors. It may benefit law enforcement and intelligence agencies to develop and refine measures to better detect ideologically motivated cyberattacks, regardless of the degree to which they are backed by nation-states. Such measures could improve the proactive detection of online threats across all types of targets.

At the same time, this data was based on open-source reporting of known incidents which may not be as reliable or accurate as closed sources available to law enforcement and intelligence agencies. This may account for the generally low visibility of many forms of SAR evident in the data. More research is needed to understand the degree to which missing information is evident in both physical and cyberattack cases. Identifying the degree to which indicators are missing across both activity types could improve our

understanding the of the ways in which cyber and physical acts of extremism differ and the challenges in assessing suspicious activity indicators from open sources in general. Research is also needed to assess the extent to which fusion centers and intelligence entities currently capture measures for cyberattacks relative to traditional physical violence and the ways that this shapes proactive threat detection.

References

Department of Homeland Security. (2009). *Leftwing extremists likely to increase use of cyberattacks over the coming decade.* Washington, D. C.: Department of Homeland Security. https://irp.fas.org/eprint/leftwing.pdf

Freilich, J. D., Chermak, S. M., Belli, R., Gruenewald, J., & Parkin, W. S. (2014). Introducing the United States extremis crime database (ECDB). *Terrorism and Political Violence*, *26*(2), 372-384.

Holt, T. J., Chermak, S. M., Freilich, J. D., Turner, N., & Greene-Colozzi, E. (2022). Introducing and Exploring the Extremist Cybercrime Database (ECCD). *Crime & Delinquency*, 00111287221083899.

SAR Indicator	Total	Nation-State
Group associations	127	68
Hacking attempts	111	62
Joining or creating groups	95	50
Technology concealment behaviors	59	38
Research and planning	59	40
Religious political justifications	58	29
Breached a similar site	56	35
Mobilizing others to the cause	51	31
Fraud	43	32
Impersonation attempt	43	29
Altering social media	43	31
Economic cybercrime	38	28
Dehumanizing targets	36	20
Collecting intelligence about the target	33	14
Attempted to breach a site	30	22
Violent participation	29	0
Communicating with violent extremists	29	7
Radicalizing others	28	20
Evading law enforcement	25	15
Financial manipulation or crime	24	12
Collecting intel about the target via cyber	24	14
Presenting false information to gain access	23	17
Presenting false identification to gain access	21	12
Communicating a threat to engage in a cyberattack against a site	20	10
Apps to facilitate attack	19	13
Website defaced	18	4
Encouraging violence	17	3
Producing violent media content	17	13
Money laundering	17	8
Praising attacks	16	7
Leaked intent	15	0
Online video for training	15	0
Engaging in social engineering in physical space	14	3
Financial manipulation or crime	13	12
Theft or diversion prior to incident	10	4
Physically damaging target	10	0
Consuming extremist media	8	0
Violent acceptance	8	0

SAR Indicator	Total	Nation-State
Structuring	8	3
Engaging in suspicious travel	8	7
Relationships to violent extremists	7	0
Cryptocurrency transfers	7	3
New skill	6	4
Collected intel about attack methods	5	1
Western Union/MoneyGram	5	0
Mobilizing others to violence	4	0
Travel preparation	4	1
Suspicious credit card	3	3
Suspicious debit card	3	3
Unusual search history	3	1
More than one ideology	2	0
Asking questions or investigating cybersecurity protocols	1	0
Travel prep	1	1
Supporting terrorism financing	1	1
Obstruction of law enforcement	1	0
Desire to travel for extremist commitment	1	0
Server racks or equipment	1	1
Behavioral changes	1	0
Acquiring weapons	1	0
Building explosives	1	0
Explosive materials	1	0

Acknowledgement

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 20STTPC00001-03-01.

Disclaimer

The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.